

ABSTRACT OF THE DISCLOSURE

5       The present invention discloses a  
software-based commercial key escrow system  
(KES) for the PKI environment that enables an  
entity such as the court to monitor  
communications of users suspected of unlawful  
activities while protecting the privacy of law-  
abiding users.

10       The present invention provides a key  
escrow system providing a PKI-roaming service  
and the perfect forward secrecy to the key  
management agent (KMA).